

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-32267
(P 2 0 0 2 - 3 2 2 6 7 A)
(43) 公開日 平成14年1月31日 (2002.1.31)

(51) Int. Cl. ⁷	識別記号	F I	テマコード (参考)		
G06F 12/14	310	G06F 12/14	310	B	5B017
G11C 16/02		G11C 17/00	601	P	5B025
H01L 27/04		H01L 27/04		U	5F038
21/822					

審査請求 有 請求項の数 3 O L (全 5 頁)

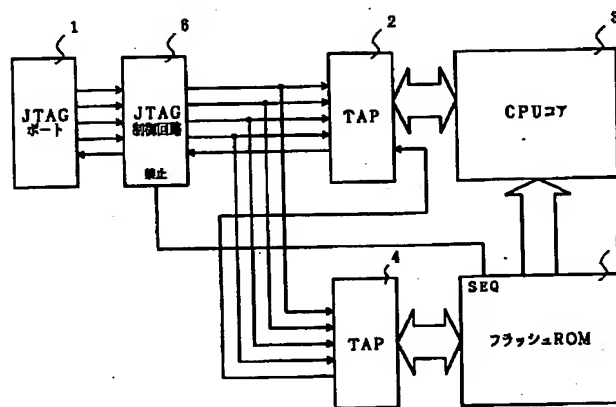
(21) 出願番号	特願2000-216983 (P 2000-216983)	(71) 出願人	591049893 株式会社 沖マイクロデザイン 宮崎県宮崎郡清武町大字木原7083番地
(22) 出願日	平成12年7月18日 (2000.7.18)	(71) 出願人	000000295 沖電気工業株式会社 東京都港区虎ノ門1丁目7番12号
		(72) 発明者	新森 信明 宮崎県宮崎郡清武町大字木原7083番地 株 式会社沖マイクロデザイン内
		(74) 代理人	100089635 弁理士 清水 守 (外 2 名)
		F ターム (参考)	5B017 AA03 BA04 BA09 BB09 CA12 5B025 AD14 AE10 5F038 BH01 BH20 DF11 EZ20

(54) 【発明の名称】 半導体回路

(57) 【要約】

【課題】 フラッシュROMの内容が第三者に読み出されることを防止することができる半導体回路を提供する。

【解決手段】 半導体回路において、フラッシュROM 5のセキュリティビットに“1”を書込むと、JTAGポート1を使用したフラッシュROMライタによる読出しだけでなく、JTAGポート1を使用したデバッグ機能も使用不可能となるため、フラッシュROM 5の内容が第三者に読出されることが全く無くなる。



【特許請求の範囲】

【請求項1】 JTAGポートとTAPの間にフラッシュROMのセキュリティビットで制御されるJTAG制御回路を具備することを特徴とする半導体回路。

【請求項2】 フラッシュROMのセキュリティビットとJTAG制御回路の間にインヒビットNANDゲートとマイコン汎用ポートをPinスクランブル回路にてデコードする回路を設け、前記Pinスクランブル回路の出力の逆相を前記インヒビットNANDゲートの片方に10 入力し、前記フラッシュROMのセキュリティビットの出力をもう片方に10 入力した回路を具備することを特徴とする半導体回路。

【請求項3】 フラッシュROMのセキュリティビットとJTAG制御回路の間にインヒビットNANDゲートとマイコン内部レジスタとしてデバッグイネーブルレジスタを設け、前記インヒビットNANDゲートに前記デバッグイネーブルレジスタの出力の逆相を入力し、前記フラッシュROMのセキュリティビットの出力をもう片方に10 入力した回路を具備することを特徴とする半導体回路。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、半導体回路に関するものである。

【0002】

【従来の技術】 図4はかかる従来の半導体回路としてのJTAG回路の構成図である。

【0003】 この図において、1はJTAG (Joint Test Action Group) ポート、2, 4はTAP (Test Access Port)、3はCPUコア、5はフラッシュ (Flash) ROMである。

【0004】 昨今のマイコン (マイクロコントローラ) では、JTAG等を使用したデバッグ機能が搭載されているマイコンが主流になってきている。このデバッグ機能を使用してマイコンのソフト開発者はアプリケーションソフトのデバッグを行い、容易にプログラムを開発できるようになっている。

【0005】 また、最近多くなっているフラッシュROM内蔵マイコンでは、JTAGを使用してフラッシュROMの書換えが実行できるようになっている。そして、このフラッシュROMにはセキュリティビットを設け、フラッシュROMの内容が第三者に読み出せないようになっている。因みに、フラッシュROMに書き込まれるデータは、ユーザー作成のアプリケーションプログラムであり、上記したセキュリティビットをセットすると、フラッシュROMのライタでの読み出し及び部分的な領域の書換えが不可能になる (例えば、特開平11-85620号公報参照)。

【0006】

【発明が解決しようとする課題】 しかしながら、上記した従来のフラッシュROMのセキュリティはセキュリティビットに“1”をセット後はJTAGを使用したフラッシュROMライタではフラッシュROMの内容が読み出されないようになってはいるが、JTAGを使用したデバッグ機能では、図4に示すように、JTAGインターフェースとしてのJTAGポート1のTAP2にてCPUコア3に対し直接命令を挿入できるため、フラッシュROM5の内容を容易にダウンロードできる。このためセキュリティビットの意味をなしていない。

【0007】 本発明は、上記問題点を除去し、フラッシュROMの内容が第三者に読出されることを防止することができる半導体回路を提供することを目的とする。

【0008】

【課題を解決するための手段】 本発明は、上記目的を達成するために、

【1】 半導体回路において、JTAGポートとTAPの間にフラッシュROMのセキュリティビットで制御されるJTAG制御回路を具備することを特徴とする。

20 【0009】 【2】 半導体回路において、フラッシュROMのセキュリティビットとJTAG制御回路の間にインヒビットNANDゲートとマイコン汎用ポートをPinスクランブル回路にてデコードする回路を設け、前記Pinスクランブル回路の出力の逆相を前記インヒビットNANDゲートの片方に10 入力し、前記フラッシュROMのセキュリティビットの出力をもう片方に10 入力した回路を具備することを特徴とする。

30 【0010】 【3】 半導体回路において、フラッシュROMのセキュリティビットとJTAG制御回路の間にインヒビットNANDゲートとマイコン内部レジスタとしてデバッグイネーブルレジスタを設け、前記インヒビットNANDゲートに前記デバッグイネーブルレジスタの出力の逆相を入力し、前記フラッシュROMのセキュリティビットの出力をもう片方に10 入力した回路を具備することを特徴とする。

【0011】

【発明の実施の形態】 以下、本発明の実施の形態について詳細に説明する。

40 【0012】 まず、本発明の第1実施例について説明する。

【0013】 図1は本発明の第1実施例を示す半導体回路の回路図である。

【0014】 この実施例では、JTAGポート1とTAP2, 4の間に、信号を禁止したり許可したりすることのできるJTAG制御回路6を設け、この制御をフラッシュROM5のセキュリティビットで行うように構成したものである。なお、図1において、3はCPU (中央処理装置) である。

50 【0015】 以下、この実施例の回路の動作について説明する。

【0016】プログラマーはJTAGポート1を使用してデバッグを行いプログラムの開発を行うが、プログラムの開発が終了すると、フラッシュROM5のセキュリティビット(SEQ)に“1”を書込む。セキュリティビットが“1”になるとJTAG制御回路6に禁止信号として入力され、JTAGポート1とTAP2, 4間の信号のやり取りが禁止され、結果としてJTAGポート1を使用したデバッグが使用できなくなる。つまり、JTAGポート1とTAP2, 4の間にORゲート(論理を変えればANDゲートでも可能)を挿入し、SEQ=1となったら、TAP2, 4には“1”しか入力されなくなるような回路構成にする。

【0017】このように第1実施例によれば、フラッシュROM5のセキュリティビットに“1”を書込むとJTAGポート1を使用したフラッシュROMライタによる読出しだけでなく、JTAGポート1を使用したデバッグ機能も使用不可能となるため、フラッシュROM5の内容が第三者に読出されることが全く無くなる。

【0018】次に、本発明の第2実施例について説明する。

【0019】図2は本発明の第2実施例を示す半導体回路の回路図である。なお、第1実施例と同じ部分には同じ符号を付してその説明は省略する。

【0020】この実施例ではフラッシュROM5とJTAG制御回路6のJTAG制御ポートとの間にインヒビット(INHIBIT) NANDゲート7を設け、且つマイコンの汎用ポート9をデコードするPinスクランブル回路8を設けるようにしたものである。なお、Pinスクランブル回路8は汎用ポート9のうち1本または数本をデコードし、インヒビットNANDゲート7に入力するもので、チップ毎にマスクオプション等で指定できるものである。

【0021】以下、この実施例の回路の動作について説明する。

【0022】上記した第1実施例と同様にプログラマーはデバッグ終了後にフラッシュROM5のセキュリティビットに“1”を書込み、第三者がJTAGポート1を使用したデバッグ機能によるフラッシュROM5の内容の読出しを禁止する。しかし、セキュリティ書き込み後でもチップ毎に設定されたPinスクランブル回路8で汎用ポート9をデコードすることにより、JTAGポート1でのデバッグが可能となる。

【0023】このように第2実施例によれば、フラッシュROM5のセキュリティビット書き込み後もチップ毎に設定されたPinスクランブル回路8の内容(マスクオプション等の内容)を知っているプログラマーはJTAGポート1を使用してデバッグが行えるため、セキュリティ書換え後の動作不具合や市場クレーム品等の解析が容易になる。また、Pinスクランブル回路8を知らない第三者にはJTAGポート1を使用したデバッグは使

用できないため、フラッシュROM5の内容が第三者に漏れることはない。

【0024】次に、本発明の第3実施例について説明する。

【0025】図3は本発明の第3実施例を示す半導体回路の回路図である。なお、第1実施例と同じ部分には、同じ符号を付してそれらの説明は省略する。

【0026】この実施例ではフラッシュROM5のセキュリティビットとJTAG制御回路6との間のインヒビットNANDゲート7の一つに入力されるデバッグイネーブル(DBG_EN)レジスタ10というマイコンの内部レジスタを設けるようにしたものである。

【0027】以下、この実施例の回路の動作について説明する。

【0028】上記した第1及び第2実施例と同様に、プログラマーはデバッグ終了後はフラッシュROM5のセキュリティビットに“1”を書込み、第三者によるフラッシュROM5の内容の読出しを禁止する。しかし、プログラムの一部にレジスタに“1”をセットするプログラムを用意しておき、必要に応じてそのプログラムを起動し、デバッグイネーブルレジスタ10を“1”にセットすることにより、JTAGポート1でのデバッグが可能となる。

【0029】このように第3実施例によれば、第2実施例と同様に、フラッシュROM5のセキュリティビット書き込み後もデバッグイネーブルレジスタ10のセットのプログラムを起動することにより、JTAGポート1でのデバッグが可能となる。また、第2実施例と異なりプログラムの制御するのでマスクオプション等の無駄な費用が発生しない。更に、当然デバッグイネーブルレジスタ10のセットのプログラムの起動はフラッシュROM5のプログラムの内容を理解しているプログラム開発者のみが実行できるもので、プログラムの内容を知らない第三者がデバッグイネーブルレジスタ10をセットすることはできない。

【0030】したがって、フラッシュROM5のセキュリティビット書き込み後のデバッグが容易に行え、且つ第三者がフラッシュROM5の内容をJTAGポート1でのデバッグ機能を使用して読み出すことを防止することができる。

【0031】なお、本発明は上記実施例に限定されるものではなく、本発明の趣旨に基づいて種々の変形が可能であり、これらを本発明の範囲から排除するものではない。

【0032】

【発明の効果】以上、詳細に説明したように、本発明によれば、次のような効果を奏することができる。

(1) フラッシュROMのセキュリティビットに“1”を書込むとJTAGポートを使用したフラッシュROMライタによる読出しだけでなく、JTAGポートを使用

したデバッグ機能も使用不可能となるため、フラッシュROMの内容が第三者に読み出されることが全くなくなる。

(2) フラッシュROMのセキュリティビット書込み後もチップ毎に設定されたPinスクランブル回路の内容(マスクオプション等の内容)を知っているプログラマーはJTAGポートを使用してデバッグが行えるため、セキュリティ書換え後の動作不具合や市場クレーム品等の解析が容易になる。また、Pinスクランブルを知らない第三者にはJTAGポートを使用したデバッグは使用できないためフラッシュROMの内容が第三者に漏れることはない。

(3) 上記(2)と同様にフラッシュROMのセキュリティビット書込み後もデバッグイネーブルレジスタのセットのプログラムを起動することにより、JTAGポートでのデバッグが可能となる。また、上記(2)と異なりプログラムの制御するものでマスクオプション等の無駄な費用が発生しない。また、当然デバッグイネーブルレジスタのセットのプログラムの起動はフラッシュROMのプログラムの内容を理解しているプログラム開発者のみが実行できるものでプログラムの内容を知らない第三者がデバッグイネーブルレジスタをセットすることはできない。したがって、フラッシュROMのセキュリ

ティビット書込み後のデバッグが容易に行え、且つ第三者がフラッシュROMの内容をJTAGポートでのデバッグ機能を使用して読み出すことを防止することができる。

【図面の簡単な説明】

【図1】 本発明の第1実施例を示す半導体回路の回路図である。

【図2】 本発明の第2実施例を示す半導体回路の回路図である。

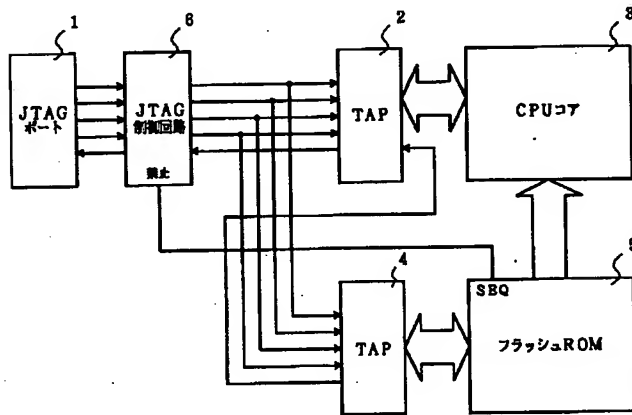
【図3】 本発明の第3実施例を示す半導体回路の回路図である。

【図4】 従来の半導体回路としてのJTAG回路の構成図である。

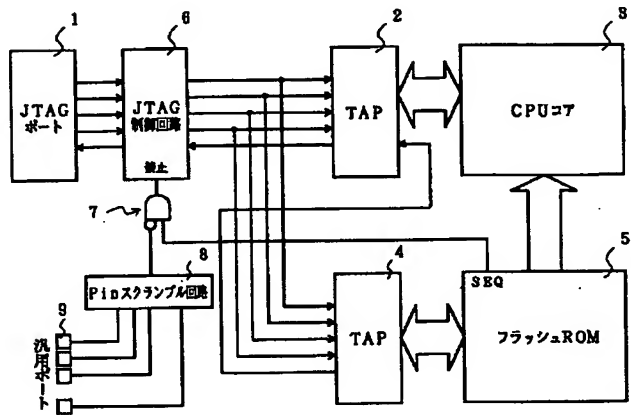
【符号の説明】

- 1 JTAGポート
- 2, 4 TAP
- 3 CPUコア
- 5 フラッシュROM
- 6 JTAG制御回路
- 7 インヒビット(INHIBIT) NANDゲート
- 8 Pinスクランブル回路
- 9 マイコンの汎用ポート
- 10 デバッグイネーブル(DBG_EN)レジスタ

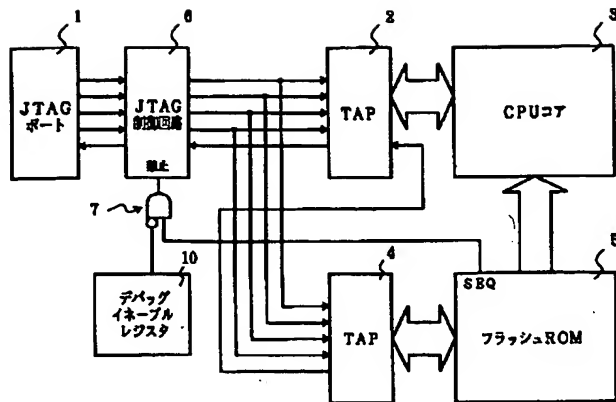
【図1】



【図2】



【図 3】



【図 4】

